REMARKS/ARGUMENTS

Claims 1, 3-5, 13-16, 18-20, 22, 23,26-30 have been rejected under 35 U.S.C. 102(e) as being anticipated by Kim et al (Kim) (US 6,701,440 B1).

The Applicant submits that Kim teaches no more than a type of virus protection acknowledged in the introduction of the present application at page 1 lines 12-21, in which email messages are scanned for known virus character strings to detect predetermined viruses. For example, Kim refers (Kim col. 2 line 12) to downloading profiles of new viruses so that the antivirus program can check for new viruses soon after new viruses are discovered. At col. 3 lines 36-37 there is a reference to "scanning the e-mail message for virus", at col. 3 lines 65-66 "a virus-detection program for scanning the e-mail message for virus", at col. 4 lines 10-11 "computer code that scans the incoming e-mail message for virus", at col. 5 lines 32-33 "the POP server scans the incoming e-mail message, including its attachments, if any, for viruses", at col. 8 lines 36-39 "the e-mail messages, including any attachments, are examined for viruses at the POP server although the e-mail message may be examined for viruses at another server, such as a virus detection server". Most significantly, at col. 9 lines 46-47 Kim teaches that "the virus detection and cleaning software is continuously updated with the discovery of new viruses". Therefore, the Applicant submits that Kim teaches a system dependent on searching for character strings associated with known viruses. The Applicant submits there is no teaching in Kim of the feature of the present invention of scanning for tags betraying the presence of operable code which may be associated with any malicious or non-malicious program code, including any known or previously unknown virus. That is, the present invention blocks emails with any operable program code, without relying on detecting known virus character strings. The present invention provides the advantage of avoiding the necessity of maintaining a database of virus character strings identifying all known viruses and provides the additional advantage of detecting previously unknown viruses. This differentiates the invention from Kim, which teaches scanning for predetermined virus character strings, not, as in the present invention for tags which, for example, mean that an electronic mail message can potentially run an

external program or trigger a program. In fact, there is no teaching whatsoever in Kim concerning such tags. In particular, there is no hint or suggestion in Kim of "scanning the electronic mail message for tags indicating the presence of operable program code" as claimed in independent claims 1 and 15, since Kim merely detects known character strings associated with known viruses.

Kim also teaches inserting a text message in a clean email message prior to forwarding the email to the destination email address (Kim col. 3 lines 57-59). There is no hint or suggestion in Kim of replacing a removed tag and operable code with alternative text, as claimed in claims 4 and 19 of the present application.

Claims 2, 6-12, 17, 21, 24 and 25 have been rejected in the light of a combination of Kim and US 5,889,943 (Ji).

Ji refers to or employs known virus scanning and detection, such as behaviour interception, signature scanning, i.e. detecting predetermined virus character strings, and performing a checksum on host programs (Ji col. 2 lines 10-29, col. 9 line 23-2, col. 17 lines 40-43, col. 20 lines 1-2). The Applicant submits Ji teaches removing viruses using such known techniques from files and messages accessed by electronic mail through a network postal node (Ji col. 1 lines 18-20). This includes anti-virus measures for electronic mail (Ji col. 2 lines 54-65). It is disclosed that "Viruses are detected and corrective action taken by a mail scanning apparatus ... The mail scanning apparatus preferably includes ... a virus analysis and treatment module for determining whether the message contains a virus" (Ji col. 3 line 60 – col. 4 line 1). In respect of electronic mail, Ji teaches (Ji col. 11 lines 54 – col. 12 line 1) that, "The present invention scans the message for portions that have been encoded with an "uuencoded" encoding scheme that encodes binary data to ASCII data, "Uuencoded" portions of messages usually start with a line like "begin 644 filename" and end with a line like "end". The existence of such uuencoded portions suggests the possibility that a file may contain viruses. This scanning for "uuencoded" portions is just one of many scanning techniques that may be used ... the present invention could be modified to scan for other encoded portions such as those encoded according to other schemes such as mime". Any encoded portion detected is decoded to convert the file

back to binary code and a virus-checking program is executed on the decoded file and scanned for viruses in a conventional manner (Ji col. 12 lines 19-29). Ji therefore merely teaches the detection and decoding of encoded electronic mail messages before performing conventional virus checking procedures. The Applicant submits there is no teaching or suggestion in Ji of the feature of claims 1 and 15 of the present invention of searching for tags betraying the presence of operable code which may be associated with any malicious or non-malicious program code, including any known or previously unknown virus. The present invention therefore provides the advantage over Ji of avoiding the necessity of maintaining a database of virus character strings identifying all known viruses, or of only detecting viruses after programs have been infected by using behaviour interception or checksums as in Ji, and provides the additional advantage of blocking previously unknown viruses. The invention therefore has the advantage of blocking new viruses and blocking unique viruses targeted at an individual recipient.

In particular, there is no suggestion in a combination of Ji and Kim of "scanning the electronic mail message for tags indicating the presence of operable program code" as claimed in independent claims 1 and 15.

As claims 1 and 15 are submitted to be allowable, it is also submitted all the claims dependent on claims 1 and 15 are also allowable. In particular, Ji teaches that where a virus is detected in an electronic mail message the system of Ji may 1) do nothing and transfer the message unchanged, 2) transfer the message with the infected parts deleted, 3) rename and store the infected portions or 4) write the output of the virus-checking program into the mail message in place of the respective encoded portions (Ji col. 12 lines 45-56). There is therefore no teaching in Ji of replacing a removed tag and operable code with alternative text, as claimed in claims 4 and 19 of the present application.

In view of the submitted remarks, it is respectfully submitted that allowable subject matter has been defined and the Examiner is requested to reconsider his prior art objections.

Application No. 09/812,409
Amendment dated:
Reply to Office Action of: August 17, 2004

Accordingly, early allowance of the subject application is earnestly requested. If the Examiner should have any queries, he is invited to contact the undersigned.

Respectfully Submitted,

Date: 11/17/04

Douglas S. Rupert, Reg. No. 44,434

SEYFARTH SHAW LLP
55 East Monroe Street
Suite 4200
Chicago, Illinois 60603-5803
Telephone: (312) 346-8000
Facsimile: (312) 269-8869

CERTIFICATE OF MAILING

I hereby certify that this paper is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 11/17/04